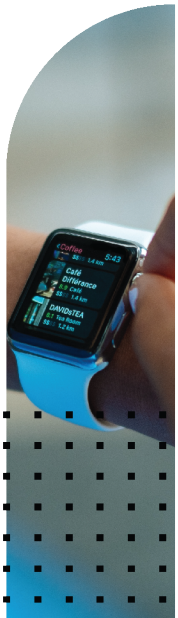
Release Notes

FortiSwitchOS 7.0.2



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 23, 2021
FortiSwitchOS 7.0.2 Release Notes
11-702-726437-20210823

TABLE OF CONTENTS

Change log

Date	Change Description
August 23, 2021	Initial release for FortiSwitchOS 7.0.2

Introduction

This document provides the following information for FortiSwitchOS 7.0.2 build 0049.

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.0.2 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424D, FS-424D-FPOE, FS-424D-POE, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448D, FS-448D-FPOE, FS-448D-POE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D-FPOE, FS-524D, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1048D, FS-1048E
FortiSwitch 3xxx	FS-3032D, FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in FortiSwitchOS 7.0.2

Release 7.0.2 provides the following new features:

- New commands allow you to specify which IGMP-snooping and MLD-snooping groups are cleared:
  - `execute clear switch igmp-snooping all`
  - `execute clear switch igmp-snooping group <multicast_IPv4_address>`
  - `execute clear switch igmp-snooping interface <interface_name>`
  - `execute clear switch igmp-snooping vlan <VLAN_ID>`
  - `execute clear switch mld-snooping all`
  - `execute clear switch mld-snooping group <multicast_IPv6_address>`
  - `execute clear switch mld-snooping interface <interface_name>`
  - `execute clear switch mld-snooping vlan <VLAN_ID>`

  You can also combine the commands for more control.
- You can now sort each column on the *Log* > *Entries* page.
- As part of the existing support for RFC 1493, the following OIDs have been added:

Name	OID
dot1dBaseBridgeAddress	.1.3.6.1.2.1.17.1.1.0
dot1dBaseNumPorts	.1.3.6.1.2.1.17.1.2.0
dot1dBaseType	.1.3.6.1.2.1.17.1.3.0
dot1dTpFdbTable TpFdbAddress TpFdbPort TpfdbStatus	.1.3.6.1.2.1.17.4.3 .1.3.6.1.2.1.17.4.3.1.1 .1.3.6.1.2.1.17.4.3.1.2 .1.3.6.1.2.1.17.4.3.1.3
dot1dBasePortTable BasePort BasePortIfIndex basePortCircuit	.1.3.6.1.2.1.17.1.4 .1.3.6.1.2.1.17.1.4.1.1 .1.3.6.1.2.1.17.1.4.1.2 .1.3.6.1.2.1.17.1.4.1.3

  NOTE: dot1dbasePortDelayeExceededDiscards (.1.3.6.1.2.1.17.1.4.1.4) and dot1dBasePortMtuExceededDiscards (.1.3.6.1.2.1.17.1.4.1.5) are not supported.
- When DHCP snooping is enabled and a DHCP server is detected on an untrusted interface, a log entry is generated, either "A rogue DHCPv6 server has been detected on the interface" or "A rogue DHCP server has been detected on the interface."
- You can now use RADIUS attributes to configure dynamic access control lists (DACLs) on 802.1x ports. DACLS are configured on a switch or saved on a RADIUS server. You can use DACLs to control traffic per user session or per port for switch ports directly connected to user clients. DACLs apply to hardware only when 802.1x authentication is successful.
- You can now specify the outer VLAN tag and COS queue number when configuring the access control list (ACL) policies on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE models.
- You can now enable or disable the learning-limit violation log in the GUI (*Switch* > *MAC Limit*).
- The MAC learning limit and the MAC learning limit violation log are now supported on the FSR-112D-POE.

- You can now specify that, when the MAC learning limit is exceeded, the interface that it is configured on will be disabled.
- You can now receive an SNMP trap message when the MAC learning limit is exceeded.
- NAC LAN segments are now supported on the FS-148F, FS-148F-POE, and FS-148F-FPOE models in FortiLink mode. FortiOS 7.0.1 or higher is required.
- You can now specify a range of multicast group addresses (IPv4) when configuring a Protocol Independent Multicast (PIM) multicast flow.
- The output of the `diagnose test authserver radius` command now includes the configured attribute-value pairs (AVPs).
- When you test the user credentials for a RADIUS server in the GUI (*System* > *Authentication* > *RADIUS*), the configured AVPs are now returned, along with the status of the connection and user credentials.
- You can now view if a module supports the diagnostic monitoring interface (DMI):
  - The output of the `get switch modules status` command reports if a module does not support DMI.
  - There is a new *DMI* column on the *Module Summary* page (*Switch* > *Monitor* > *Modules*).

Refer to the FortiSwitch feature matrix for details about the features supported by each FortiSwitch model.

Special notices

Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.

If you do not convert the admin password before downgrading from FortiSwitchOS 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

To convert the format of the admin password in FortiSwitchOS 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:

1. Enter the following CLI command to convert the admin password from SHA256 to SHA1 encryption:

   ```
   execute system admin account-convert <admin_name>
   ```

2. Downgrade your firmware.

Connecting multiple FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitchOS 7.0.2 supports upgrading from FortiSwitchOS 3.5.0 and later.

For FortiSwitch units managed by FortiGate units, refer to the *FortiSwitch Devices Managed by FortiOS Release Notes* for upgrade information. See https://docs.fortinet.com/document/fortiswitch/7.0.0/managed-switch-release-notes.

Product integration and support

FortiSwitchOS 7.0.2 support

The following table lists FortiSwitchOS 7.0.2 product integration and support information.

Web browser	• Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

Resolved issues

The following issues have been fixed in FortiSwitchOS 7.0.2. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
617755	The internal interface cannot obtain IPv6 addresses with dhcpv6-snooping enabled on the native VLAN.
701560	The DHCPv6 client cannot get the IP address when VLAN assignment is applied on the FSR-112D-POE model.
712323	After VRRP is enabled, the switch does not respond to ARP requests from the directly connected interface.
722738	The `diagnose sys pcb temp` and `diagnose sys soc temp` commands report the wrong values for the FS-224E.
726364	When a FS-108E is in FortiLink mode, VLANs are not being synchronized.
727741	Ping results in a managed switch topology are not correct.
727742	MCLAG topologies take too long to converge.
728704	The status of the MGMT interface does not reflect the physical connection.
730505	The switch host name displays only 16 characters.
732228	When configuring a DGCP server in the CLI, the description field accepts only a string of 3 characters long.
733819	When a managed switch is rebooted, nonsense characters appear in the syslog message.

Known issues

The following known issues have been identified with FortiSwitchOS 7.0.2. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
480605	When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server. **Workarounds:** —Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. —Temporarily disable dhcp-snooping on vlan, issue the `execute interface dhcpclient-renew <interface>` command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values. **Workaround:** When using the cable diagnostics feature on a port (with the `diagnose switch physical-ports cable-diag <physical port name>` CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.
542031	For the 5xx switches, the `diagnose switch physical-ports led-flash` command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.
572052	Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters. **Workaround:** Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.
606044	The value for cable length is wrong when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.

Bug ID	Description
609375	The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP Power Ethernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.
610149	The results are inaccurate for open and short cables when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
673433	Some 7-meter DAC cables cause traffic loss for the FS- 448E model.
734917	When you configure a PIM multicast flow with a range of group addresses for SVIs and the group address range overlaps with a dynamic IGMPv3 group receiver that has joined groups in a different VLAN, then the dynamic IGMPv3 receiver will still receive multicast traffic unexpectedly even after leaving the joined groups.

www.fortinet.com